Purchase Card On-Line System (PCOLS)

Frequently Asked Questions

v17 – December 2009

Agenda

- Expectations
  - Provide review of key concepts
  - Address specific issues of known interest
- Executive Summary
- PCOLS Components
- Enterprise Monitoring and Management of Accounts (EMMA) Detailed Overview
- Authorization, Issuance and Maintenance (AIM) Detailed Overview
- Frequently Asked Questions (FAQs)
  - Policy FAQs
  - EMMA FAQs
  - AIM FAQs
  - Data Mining / Risk Assessment FAQs

Executive Summary

- How we got here:
  - Government Accountability Office (GAO) audit reports
  - DoD and Service Inspector General (IG) reports (600 - 800 since 1999)
  - Comptroller DoD Management Information Directive (MID) 904 directed approximately 50 actions, including:
    - *Develop methods to ensure controls over charge cards*
    - *Develop data mining tool to identify misuse of charge cards*
- PCOLS is a response to Congressional / GAO mandate to:
  - Capture the full Purchase Card hierarchy
    - *Reestablish Supervisors into reconciliation review process*
  - Improve internal controls
  - Audit data using the Common Access Card (CAC)
  - Mine transactions for fraud and misuse
  - Integrate the Purchase Card into other Department e-business applications
  - Facilitate transition to “new” Purchase Card issuing banks

PCOLS Components

- **Enterprise Monitoring and Management of Accounts (EMMA)**
  - Used to provision users into roles in a hierarchy
  - Based on roles, grants access to the other PCOLS applications

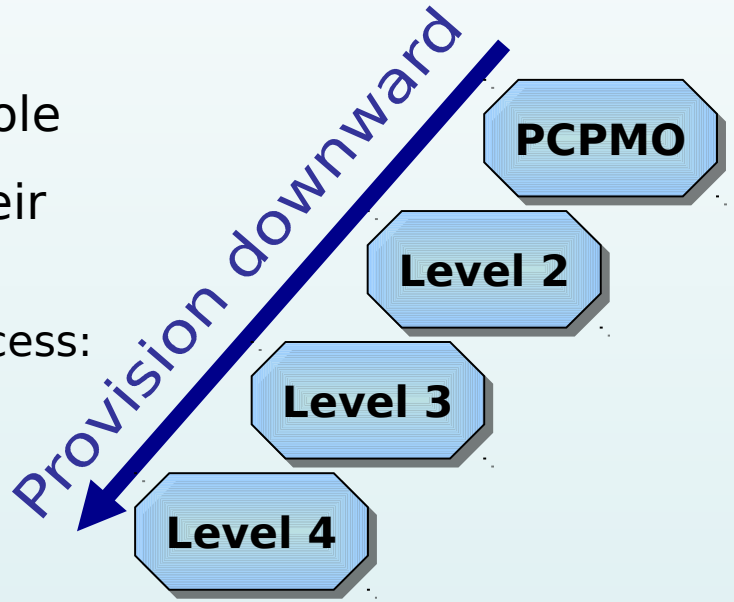
- **Authorization, Issuance and Maintenance (AIM)**
  - System to issue and maintain Managing Accounts (MA) and Cardholder Accounts (CA)
  - Interfaces with the (currently) two banks
  - Store account information

- **Data Mining (DM)**
  - Developed by third party vendor (HNC)
  - Reviews all transactions of all CAs and flags any considered misuse or fraudulent
  - Flagged transactions are to be reviewed and verified of validity by users

- **Risk Assessment (RA)**
  - Developed by third party vendor (PWC)
  - Reports an organization's "health" in the Purchase Card Program
    - *Health depends on number of misuse/fraudulent cases and other factors*

EMMA Detailed Overview

- Captures hierarchies to grant system access to authenticated users
  - The hierarchy incorporates Supervisors into the program
- Uses the CAC to link an individual to a role
- Allows individuals to add roles under their own, to continue down the hierarchy
  - Provisioning – an iterative three step process:
    - *Create organization*
    - *Create role within organization*
    - *Populate role with a user*
- Other systems, such as AIM, use the roles in EMMA to grant permissions within the applications



AIM Detailed Overview

- A workflow tool used to perform various Purchase Card Program account issuance and maintenance functions such as:
  - Updating Purchase Limits
  - Changing Merchant Category Codes (MCCs)
  - Ensuring that ongoing training requirements are met
  - Ensuring that lines of accounting are current

- Draws from hierarchies recorded in EMMA to determine who has responsibility and permission to initiate and approve requests for Account issuance and maintenance
- A live interface with the bank systems allows Account requests to be sent electronically
- Daily feeds from the bank systems allows both systems to be up to date with the current Account information
- Does not replace any existing systems to review and approve card transactions

Frequently Asked Questions

Policy FAQ Table of Contents

- What is the implementation timeline for PCOLS?
- How do I obtain help with a PCOLS problem? **(2 slides)**
- Do I still use the bank online system if I am using PCOLS? Why?
- Does PCOLS duplicate any aspects of the bank's online system?
- How do I find all of my GPC organization members if they are not centrally located?
- Is my access to PCOLS affected if I replace my CAC?
- Is PCOLS NMCI Approved?
- Can we have CAC readers at home?
- Will we be able to bypass the approval hierarchy if someone is on leave, or in an emergent situation?
- How will PCOLS be mandated to afloat units where bandwidth/internet burden exists?
- What is the plan for leadership buy-in?

EMMA FAQ Table of Contents

- How should I structure my hierarchy in EMMA?
- How many users can be provisioned per role within a given EMMA organization?
- Do I have to include supervisors in my EMMA organization?
- How do I identify the proper supervisors to provision in EMMA?
- Why am I receiving emails from no_reply@dmdc.osd.mil?
- What roles do not have log-in access to EMMA?

AIM FAQ Table of Contents

- Why do I need to update my profile in AIM?
- How do I update my profile in AIM? (2 slides)
- Where do I obtain verification that required training has been c ompleted?
- What is the difference between an Office Name and an Organizat ion Name in AIM?
- As an A/OPC, am I giving up control in my organization by using AIM?
- Does PCOLS have the ability to attach training certificates and/o r appointment letters to an account request to send to the bank ?
- As a cardholder, how do I log-in to AIM?
- Does an email always accompany a task?
- Why am I receiving account update e-mail messages?

DM/RA FAQ Table of Contents

- **Will I be able to complete audits and include comments of findings in PCOLS?**
- **How will PCOLS affect surveillance?**
- **Will PCOLS replace the NAVY Program Audit Tool (PAT) system?**

Policy

Policy FAQ

- What is the implementation timeline for PCOLS?

DoD Acquisition Technology & Logistics (AT&L) requires that PCOLS implementation be complete across DoD by 4 January 2010. By this date, no cards will be issued unless through PCOLS.

For components, under the cognizance of the Director of National Intelligence (DNI), the targeted deployment date is not later than 3 January 2011.

Please see the latest Memorandum for PCOLS dated 19 November 2008 by clicking the link below:

19 November 2008 - PCOLS Memorandum

Policy FAQ

- How do I obtain help with a PCOLS problem?

PCOLS help and support is available through the following methods:

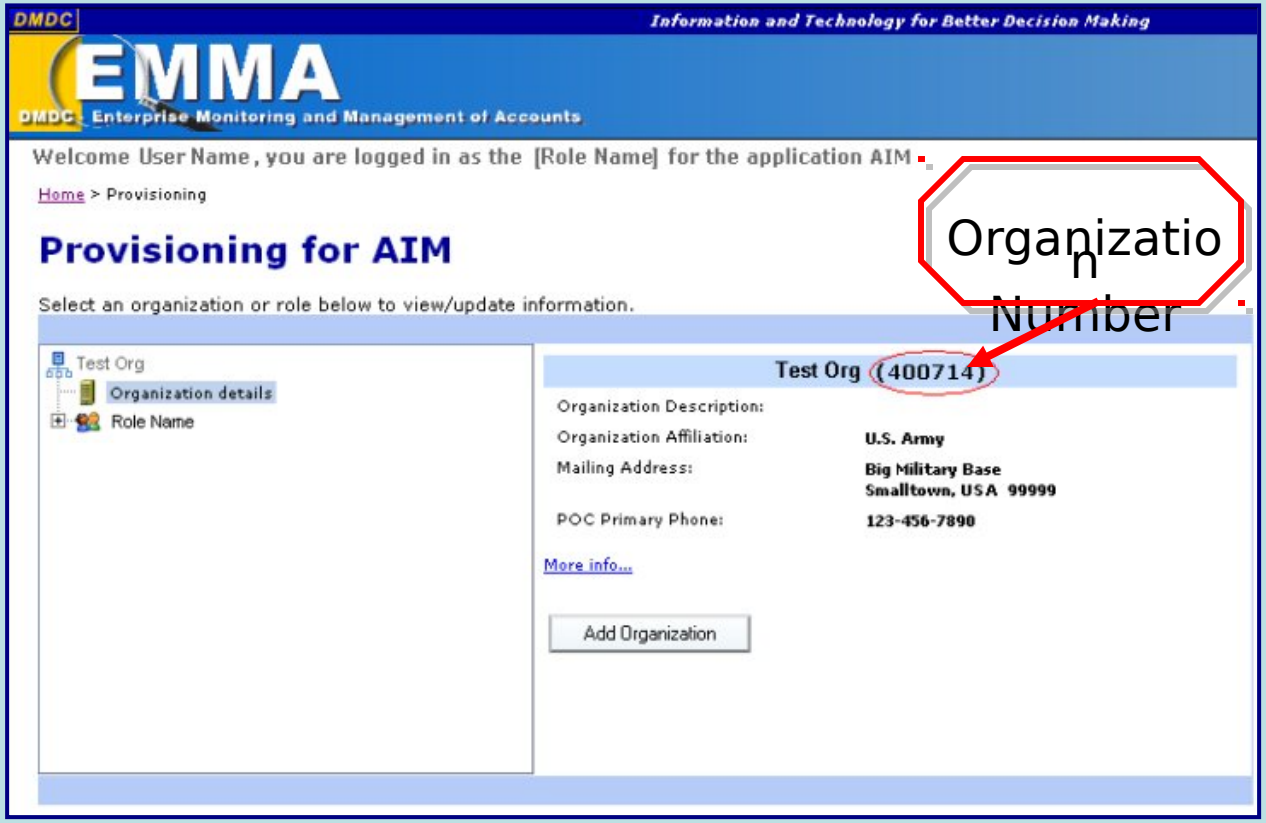
1. **Website**:
   - http://www.acq.osd.mil/dpap/pdi/eb/ebusiness_policy_support_center.html
   - Frequently Asked Questions (FAQs)
   - User Manuals (EMMA, AIM)
   - Site Deployment Packet
   - Webinar Schedule

2. **Phone**:
   - 800-376-7783, Direct Dial 269-961-7307, DSN 661-7307
   - *Operation hours: 24 x 7*

3. **Email**: dlacontactcenter@dla.mil

Note: Include organization number in all help desk communications (see next page).

- How do I obtain help with a PCOLS problem? *(cont'd)*


DMDC
Information and Technology for Better Decision Making
EMMA
DMDC Enterprise Monitoring and Management of Accounts
Welcome User Name, you are logged in as the [Role Name] for the application AIM
Home > Provisioning
Provisioning for AIM
Select an organization or role below to view/update information.
Organization Number
Test Org
Organization details
Role Name
Test Org (400714)
Organization Description:
Organization Affiliation: U.S. Army
Mailing Address: Big Military Base
Smalltown, USA 99999
POC Primary Phone: 123-456-7890
More info...
Add Organization

When contacting either the DMDC help desk or the PCOLS Help Desk, ensure that the organization number is available, along with the caller's name, contact information, and a description of the problem.

Policy FAQ

- Do I still use the bank online system if I am using PCOLS? Why?

Yes.

PCOLS is used to manage the Purchase Card Program from an account level, encompassing issuance and maintenance requests for Managing and Cardholder accounts.

Systems such as Access On-Line and Citidirect are used to look at transaction-level details for Purchase Card accounts.

Policy FAQ

- Does PCOLS duplicate any aspects of the bank's online system?

Yes.

However, as PCOLS implementation continues, the duplicity will be removed.

Policy FAQ

- How do I find all of my GPC organization members if they are not centrally located?

In the case where there is already a GPC organizational structure in place, use that structure. Ensure that the supervisors for the Cardholder, A/BO, and A/OPC are included. If you are unsure who should fill these roles, contact your supervisor.

In the case where the GPC organizational structure has not been defined or two or more roles are occupied by a single individual, a comprehensive organizational hierarchy should be created prior to provisioning in EMMA.

Policy FAQ

- Is my access to PCOLS affected if I replace my CAC?

Replacing your CAC will have no impact within PCOLS.

The link between your CAC identity and the established access and roles within EMMA and AIM are not affected if your CAC is lost and/or replaced. The unique identification of the new CAC is automatically associated to that of the old CAC within PCOLS.

Policy FAQ

- Is PCOLS NMCI Approved?

Yes.

PCOLS is certified for use within Navy Marine Corps Intranet (NMCI). The term "certification" refers to the process by which applications/systems are determined or made to be compatible with the NMCI network and its information assurance infrastructure.

Policy FAQ

- Can we have CAC readers at home?

Many Department of Defense (DoD) organizations utilize the ActivCard USB Common Access Card (CAC) readers. The CAC readers, in conjunction with the user's Smart Card, enable access to DoD PKI-enabled websites and allow the user to send signed and encrypted email utilizing the DoD Public Key Infrastructure (PKI). If your Command is willing to provide the software and hardware you can gain access to PCOLS at home.

Policy FAQ

- Will we be able to bypass the approval hierarchy if someone is on leave or in an emergent situation?

No.

PCOLS is designed so that each role has a level of accountability. PCOLS does not allow a workflow step to be bypassed.

To help facilitate leave of absence or emergent situations, PCOLS allows certain roles to have associated pool members. These pool members can assume responsibility for day-to-day PCOLS tasks.

Resource Managers: You may wish to provide an office email address to your Approving / Billing Officials to enter into the RM nomination field when establishing Managing Accounts in AIM. By using an office email address, you can avoid the scenario where a particular RM may be on leave and can not redeem the AIM token.

Policy FAQ

- How will PCOLS handle any existing bandwidth/internet burden issues?

The PCPMO will work with the appropriate departments to resolve all issues.

Policy FAQ

- What is the plan for leadership buy-in?

The PCPMO involves upper-level management in Senior Focus Groups and IPTs to inform them of the updates on the program and elicit feedback.

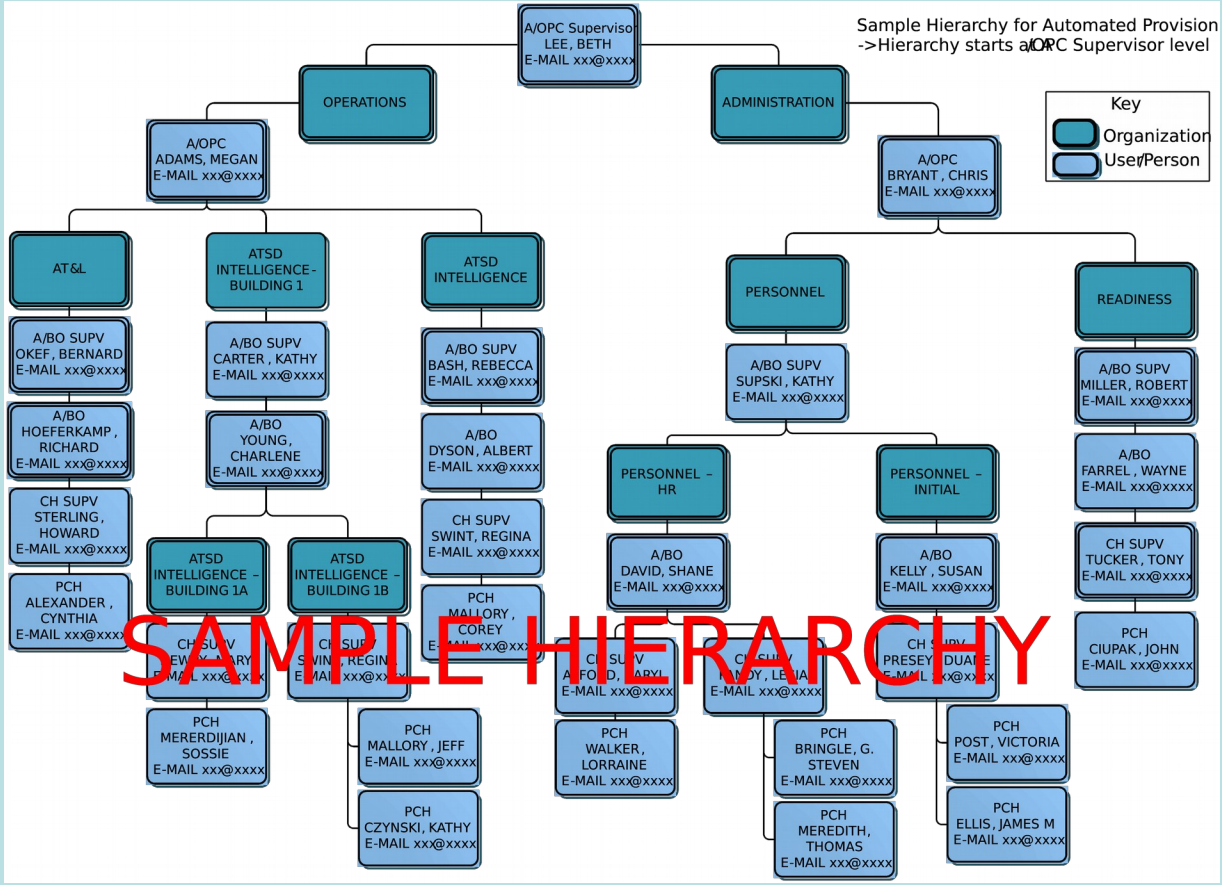
EMMA

EMMA FAQ

- How should I structure my hierarchy in EMMA?

To the right is an example hierarchy structure that can be used to help develop your own hierarchy structure for your particular organization.

The PCOLS Help Desk can help guide you through the process of development.



EMMA FAQ

- How many users can be provisioned per role within a given EMMA organization?

EMMA currently allows for the following number of users per role within a given organization:

Role Name	# of users	Role Name	# of users
AEA - Level 2	10	Component RM	10
HCA Agent - Level 3	10	Major RM	10
High-Level A/OPC	30	Intermediate RM	10
A/OPC Supervisor	30	RM Supervisor	1
A/OPC	30	RM	3
A/BO Supervisor	5	RM Pool	100
A/BO	100		
Cardholders Supervisor	100		

EMMA FAQ

- Do I have to include supervisors in my EMMA organization?

Yes.

Supervisors within a GPC organization have always been designated with the responsibility to provide supervisory oversight for their GPC organizations. PCOLS provides a level of rigor in the system to ensure that supervisors are involved to the degree required. The Cardholders Supervisor and A/BO Supervisor are necessary to ensure successful AIM workflow operations and possess responsibility for supervisory oversight within their GPC organizations.

EMMA FAQ

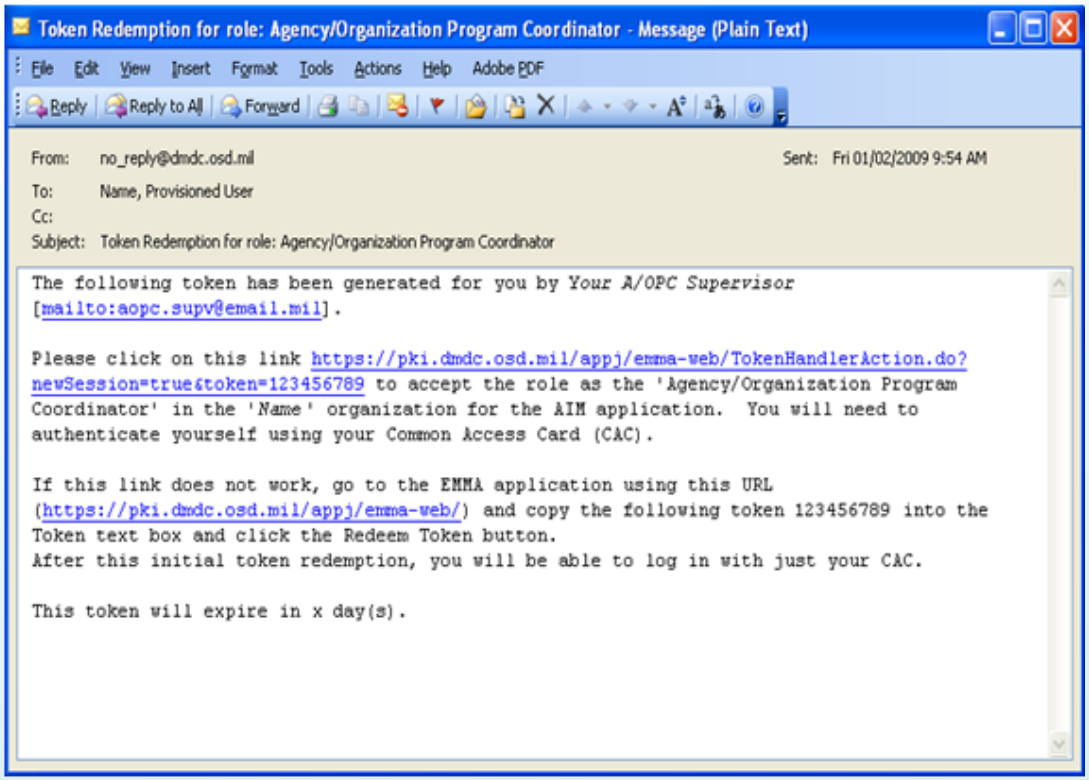
- How do I identify the proper supervisors to be provisioned in EMMA?

The supervisor who conducts the performance appraisal for the Cardholder, A/BO, or A/OPC would be the appropriate PCOLS supervisor to be provisioned in EMMA.

EMMA FAQ

- Why am I receiving emails from no_reply@dmdc.osd.mil?

All PCOLS system email messages originate from no_reply@dmdc.osd.mil and many of these require the recipient to take specific actions (e.g., EMMA and AIM token messages). Please ensure that all Purchase Card personnel are aware that these messages are completely safe and should be thoroughly read and acted upon, as appropriate.


Token Redemption for role: Agency/Organization Program Coordinator - Message (Plain Text)
File Edit View Insert Format Tools Actions Help Adobe PDF
Reply Reply to All Forward
From: no_reply@dmdc.osd.mil
Sent: Fri 01/02/2009 9:54 AM
To: Name, Provisioned User
Cc:
Subject: Token Redemption for role: Agency/Organization Program Coordinator
The following token has been generated for you by Your A/OPC Supervisor [mailto:aopc.supv@email.mil].
Please click on this link https://pki.dmdc.osd.mil/appj/emma-web/TokenHandlerAction.do?newSession=true&token=123456789 to accept the role as the 'Agency/Organization Program Coordinator' in the 'Name' organization for the AIM application. You will need to authenticate yourself using your Common Access Card (CAC).
If this link does not work, go to the EMMA application using this URL (https://pki.dmdc.osd.mil/appj/emma-web/) and copy the following token 123456789 into the Token text box and click the Redeem Token button.
After this initial token redemption, you will be able to log in with just your CAC.
This token will expire in x day(s).

EMMA FAQ

- What roles do not have log-in access to EMMA?

Cardholders Supervisors and Resource Manager Pool Members do not have log-in access to EMMA but must be provisioned in EMMA by accepting their EMMA tokens.

Cardholders do not have log-in access to EMMA and are not provisioned in EMMA. Cardholders are tied to specific Cardholder Accounts in AIM.

AIM

AIM FAQ

- Why do I need to update my profile in AIM?

AIM uses the personal data from your Common Access Card (CAC) and the DEERS database that allows it to function as designed. This information is displayed on the AIM profile tab.

Important information that users should verify on the AIM Profile tab:

- Email address associated with CAC
- Work address stored in DEERS

Notification messages and task emails are sent to the email address associated with your CAC. If the email address is incorrect, the notifications will not be received, which could delay required task actions.

A/OPCs, A/BOs, and Cardholders are required to verify their work address to ensure successful delivery of any requested Purchase Cards or convenience checks. The work address field must be populated and will be verified with the United States Postal Service to ensure that it is valid.

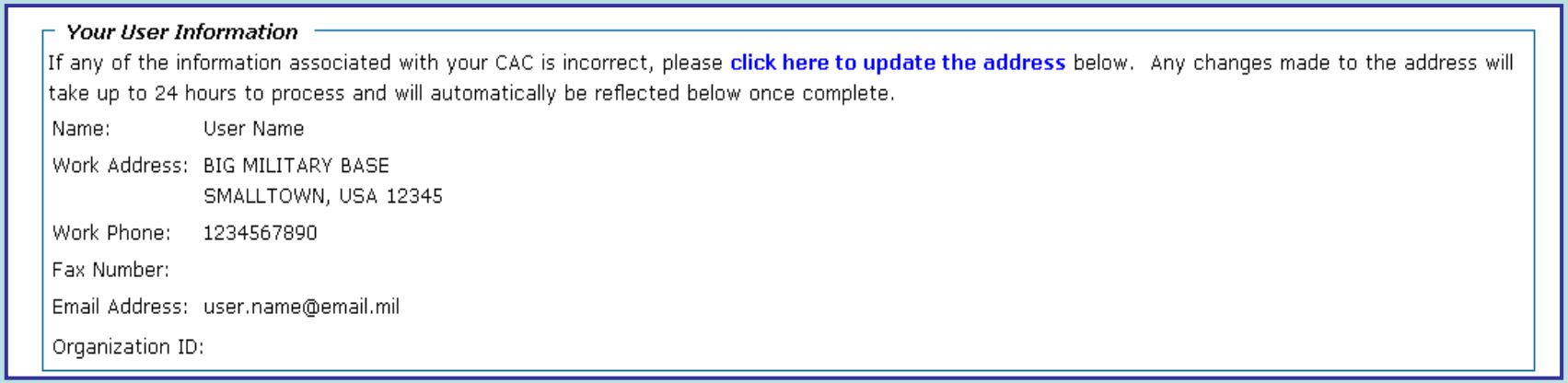
AIM FAQ

- How do I update my profile in AIM?

The AIM user profile can be accessed by clicking on the **Profile** tab.

To update your work address, click the link entitled **click here to update the address** within the AIM system text or navigate to: https://www.dmdc.osd.mil/appj/address/

To update your email address, navigate to: https://www.dmdc.osd.mil/ump/



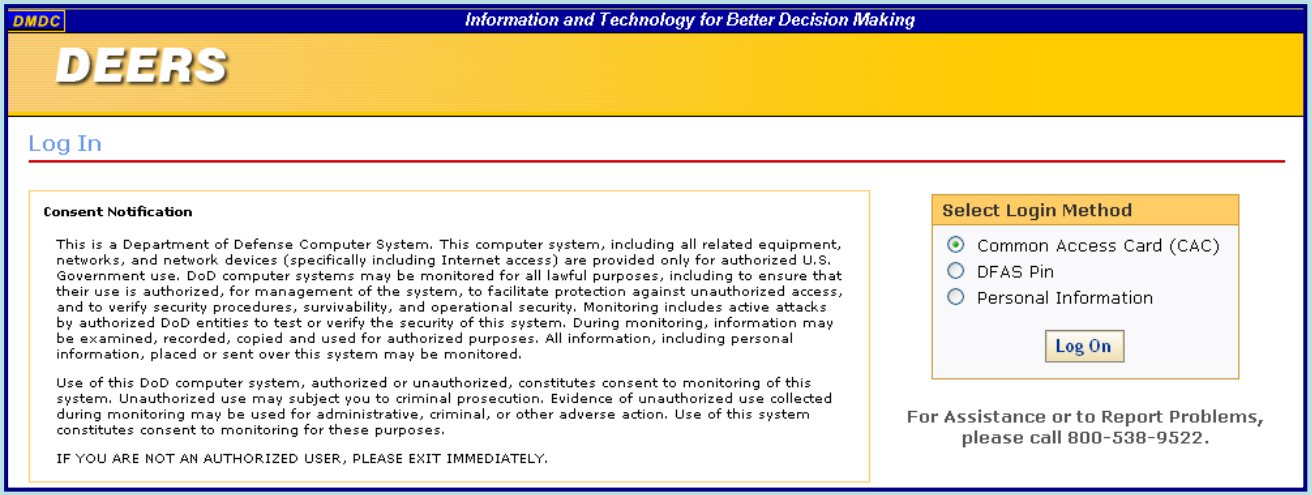
Your User Information

If any of the information associated with your CAC is incorrect, please **click here to update the address** below. Any changes made to the address will take up to 24 hours to process and will automatically be reflected below once complete.

Name:	User Name
Work Address:	BIG MILITARY BASE SMALLTOWN, USA 12345
Work Phone:	1234567890
Fax Number:	
Email Address:	user.name@email.mil
Organization ID:	

- How do I update my profile in AIM? *(cont'd)*

Your User Information is populated from your Defense Enrollment Eligibility Reporting System (DEERS) profile. The **click here to update the address** link will direct you to the DEERS Address Update site, which is a DMDC application. Any changes that are made will take effect once you log out of AIM and log back in to AIM. If you have any problems logging in or updating your address, contact the help desk shown in the Address Update application.


DMDC
Information and Technology for Better Decision Making
DEERS
Log In
Consent Notification
This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.
Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.
IF YOU ARE NOT AN AUTHORIZED USER, PLEASE EXIT IMMEDIATELY.
Select Login Method
Common Access Card (CAC)
DFAS Pin
Personal Information
Log On
For Assistance or to Report Problems, please call 800-538-9522.

AIM FAQ

- Where do I obtain verification that required training has been completed?

Currently, verification is accomplished by the A/OPC receiving the appropriate hardcopy certifications.

In the future it is anticipated that training certification from Defense Acquisition University (DAU) will be automatically linked to AIM.

AIM FAQ

- What is the difference between an Office Name and an Organization Name in AIM?

The **Office Name** in AIM is used as another method (such as account number) to identify individual Managing and Cardholder Accounts. The name is specific to the AIM application and should not be used as a substitute for the account number when communicating with the bank.

The **Organization Name** in AIM is imprinted on the Purchase Card and appears on the billing statement for the account. The AIM Organization Name is not to be confused with the EMMA Organization Name, which is used to associate a user in a hierarchical structure.

It is recommended that the Office Name be unique for each account in AIM in order to identify accounts by the Office Name. For instance, if you have multiple Purchase Cards and do not remember the account number you can reference the Office Name instead.

AIM FAQ

- As an A/OPC, am I giving up control in my organization by using AIM?

No.

The A/OPC has the final oversight and approval responsibility. In AIM, the A/OPC reviews and approves all requests prior to submitting them to the bank.

AIM uses the Purchase Card hierarchy defined in EMMA to assign specific responsibilities and tasks to designated roles within the GPC organization. In some organizations, A/OPCs have traditionally accomplished all or most of these actions themselves. By distributing specific tasks to other GPC organization members, an enhanced level of situational awareness and supervisory oversight can be attained, improving management control of the entire organization.

AIM FAQ

- Does PCOLS have the ability to attach training certificates and/or appointment letters to an account request to send to the bank?

No.

PCOLS does not have the ability to attach a document to any request transmitted to the bank. You should keep a file copy of the letters of appointment or any other documentation.

AIM FAQ

- As a Cardholder, how do I log-in to AIM?

A Cardholder does not have log-in access to AIM.

The only way a Cardholder can interface with AIM is through the use of an AIM Cardholder Nomination Token. This token is assigned by the Approving / Billing Official (A/BO) and will be delivered to the Cardholder via an e-mail message.

Once received, an AIM Cardholder Nomination Token can only be used once. All future attempts to click on the token-embedded link will result in an “Expired Token” error message. If a Cardholder does not successfully complete the Cardholder Nomination in AIM after clicking on the token, the Cardholder must contact his or her Approving / Billing Official (A/BO) or Agency / Organization Program Coordinator (A/OPC) to obtain a new AIM Cardholder Nomination Token.

AIM FAQ

- Does an email always accompany a task?

Yes.

An email is the sole notification mechanism to alert individuals involved in the AIM workflow process that a task awaits their attention. In addition, there are occasions when a notification email without an associated task is sent to involved individuals in the workflow process.

AIM FAQ

- Why am I receiving account update e-mail messages?

These are only informational e-mail messages (the subject line includes the text “PCOLS Notice”) to let you know that your account was updated by a batch process to ensure that the bank data and the AIM data are in sync with each other. If the financial data associated with your accounts is updated by the bank on a yearly basis, you will receive an account update e-mail message for each account that has been updated in the bank system.

```
From: noreply@dmdc.osd.mil [mailto:noreply@dmdc.osd.mil]
Sent: Monday, October 19, 2009 12:35 PM
To: John.Doe@us.af.mil
Subject: [PCOLS Notice] Cardholder Account Bank update

The following Cardholder Account has been updated to match the information in the bank's system:

Office Name: Not Available
Justification: Not Available
Account Number: ************7777

If you require assistance, contact the eBPSC help desk at 877-376-5787 or
mailto:defensepolicysupport@ebpsc.org.

AIM Logon: https://pki.dmdc.osd.mil/appj/aim/index.jsp
```

DM/RA

- Will I be able to complete audits and include comments of findings in PCOLS?

Yes.

Data Mining will allow authorized users to complete audits and include comments on the findings.

DM/RA FAQ

- How will PCOLS affect surveillance?

Surveillance will continue to be performed as done today, until the Data Mining/Risk Assessment piece of PCOLS has been fully deployed.

- Will PCOLS replace the NAVY Program Audit Tool (PAT) system?

Yes.

PCOLS will eventually replace PAT, when the Data Mining/Risk Assessment portion of PCOLS has been fully deployed.